

AO 91 (Rev. 11/11) Criminal Complaint

114

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

United States of America)

v.)

United States of America)

v.)

Christopher E. Pelloso)

1770 Roxbury Dr.)

Defendant(s)

Case No.

2:13-MJ-394

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of October 10, 2012 to July 8, 2013 in the county of Franklin in the
Southern District of Ohio, the defendant(s) violated:

Code Section

18 U.S.C. Section 2252

Offense Description

Receiving visual depictions of minors engaged in explicit sexual activity via the Internet

This criminal complaint is based on these facts:

See attached Affidavit incorporated by reference herein

☒ Continued on the attached sheet.


Complainant's signature

JOHN L PRIEST HSI- TFO

Printed name and title

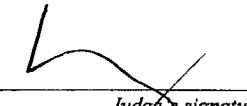
Sworn to before me and signed in my presence.

Date:

7/24/2013

City and state:

Columbus, Ohio



Judge's signature

N M King USM Judge

Printed name and title

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT, EASTERN DIVISION OF OHIO**

In the Matter of the Criminal Complaint:

United States of America

v.

Christopher E. Pelloso

1770 Roxbury Dr.

Upper Arlington, Ohio 43212

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI) Task Force Officer (TFO) John L. Priest, being first duly sworn, hereby depose and state as follows:

1. I, ICE/HSI TFO John L. Priest (your affiant) of the Franklin County Ohio Sheriff's Office, Internet Crimes Against Children Task Force, make this affidavit in support of a criminal complaint to arrest Christopher Edward Pelloso for violation of Title 18 United States Code Section 2252(a)(2) – Receipt of Child Pornography. Since this affidavit is being submitted for the limited purpose of securing a criminal complaint and arrest warrant, your affiant did not include each and every fact known concerning this investigation. Your affiant did not withhold any information or evidence that would negate probable cause. Your affiant set forth only the facts that are believed to be necessary to establish probable cause that Christopher Edward Pelloso committed the violation listed above.
2. Your affiant has been employed by the Upper Arlington Police Department since December of 1988. Since June of 2009, your affiant has been assigned to the Franklin County Special Investigations Unit conducting online child enticement and child pornography investigations as part of an Internet Crimes Against Children Task Force. Your affiant has received specialized training in the area of internet crimes involving child exploitation and child pornography. Your affiant has been involved in more than 100 investigations involving internet crimes against children, which have resulted in numerous felony arrests and convictions. Your affiant was trained and certified by ICE/HSI as a federal task force officer to conduct child exploitation investigations involving federal criminal statutes, such as Title 18 USC § 2252.
3. During the month of October 2012, Detective Rick Steller with the Franklin County Internet Crimes Against Children Task Force, was conducting online investigations to detect possible possession, receipt and distribution of child pornography offenses. On October 10, 2012, during an investigation of online peer-to-peer (p2p) file sharing programs, a computer located at IP address 99.22.72.212 was observed in a law enforcement database as a potential candidate for download of suspected child pornography, based on the Hash values and/or the titles of the files that were being shared on the computer. The IP address was observed on the eDonkey network,

a file sharing network that is available for free over the internet.

4. On October 10, 2012, Detective Steller observed a file on the computer located at IP address 99.22.72.212. This file was being shared on the eDonkey network and was observed to have a Hash value of 7F0C488C5A1630F7ED749EB40E618438. A Hash value is a unique value assigned to a file that identifies the specific file. This value has been referred to as a digital fingerprint, due to the unique nature of Hash values. Any minor change to a digital file would change the Hash value, thus two files that have the same Hash value are identical files. Detective Steller was not able to download any files from the computer at the suspect IP address on this date.

5. Detective Steller located the file with an identical Hash value in a database that has been compiled and maintained by law enforcement from previous investigations. The file was examined and it was found to be a movie of a pre-pubescent female approximately 7 years old fondling a male penis and an adult male fondling the girls genitals. The girl then performs oral sex with the adult male.

6. On October 14, 2012 during an investigation of online peer-to-peer (p2p) file sharing programs, a computer located at IP address 99.22.72.212 was again observed in a law enforcement database as a potential candidate for download of suspected child pornography, based on the Hash values and/or the titles of the files that were being shared on the computer. The IP address was again observed on the eDonkey network.

7. Detective Steller determined that the suspect IP address was owned by AT&T Internet Services. Detective Steller sent two subpoenas to AT&T Internet Services requesting subscriber information for the IP address 99.22.72.212 at the dates and times that the IP address was observed on the law enforcement database in possession of child pornography files. Detective Steller received a response from AT&T Internet Services indicating that the subscriber for IP address 99.22.72.212 is Chris PELLOSKI, 1770 Roxbury Dr., Upper Arlington, Ohio 43212.

8. Between March 29, 2013 and July 8, 2013 during investigations of online peer-to-peer (p2p) file sharing programs, a computer located at IP address 107.205.38.14 was observed in a law enforcement database as a potential candidate for download of suspected child pornography, based on the Hash values and/or the titles of the files that were being shared on the computer. The IP address was observed on the eDonkey network.

9. On April 1, 2013, Detective Steller observed that the computer at IP address 107.205.38.14 was in possession of a file with a Hash value of 8E0F8E4E977A92197D0495C927B8C765. Detective Steller was not able to download the file from the computer at the suspect IP address, but was able to locate the file with an identical Hash value in a database that has been compiled and maintained by law enforcement from previous investigations. The file was examined and it was found to be a movie that depicts two pre-pubescent females approximately 6 and 8 years old, using a foreign object to penetrate the vaginas of each other. One of the girls then performs oral sex with the adult male.

10. Detective Steller determined that the suspect IP address was owned by AT&T Internet Services. Detective Steller sent a subpoena to AT&T Internet Services requesting subscriber information for the IP address 107.205.38.14 at the date and time that the IP address was observed by the law enforcement database in possession of child pornography. Detective Steller received a response from AT&T Internet Services indicating that the subscriber for IP address 107.205.38.14 is Jamie Blackman, 1770 Roxbury Dr., Upper Arlington, Ohio 43212.

11. On July 16th, 2013, your affiant obtained a state search warrant for 1770 Roxbury Dr., Upper Arlington, Ohio 43212 signed by a Franklin County Municipal Judge. On July 16th, 2013, your affiant, along with other members of the Internet Crimes Against Children Task Force, executed the search warrant at 1770 Roxbury Dr., Upper Arlington, Ohio 43212

12. During the execution of the search warrant, Task Force Officers recovered numerous computers and digital media from the residence. Included among the evidence recovered was an HP Pavilion desktop computer. This computer was recovered from a bedroom that was determined to be Christopher E. PELLOSKI'S.

13. During the execution of the search warrant, your affiant conducted a forensic preview of the HP Pavilion desktop computer that was recovered from 1770 Roxbury Dr. Multiple images of child pornography were observed during this brief preview, including images that depicted preteen girls in various states of undress with the focal point on the genitals. Your affiant also observed images that appeared to depict minor family members of the PELLOSKI family in a state of undress.


14. On July 16th, 2013 Detective Steller learned that Chris PELLOSKI was in Boulder, Colorado with a laptop computer that belongs to Ohio State University. Detective Steller made contact with Christopher PELLOSKI by telephone and interviewed him. PELLOSKI admitted that he was responsible for downloading child pornography using the HP Pavilion desktop computer. PELLOSKI also informed Detective Steller that he had used a laptop computer belonging to Ohio State University to download child pornography and that he had the laptop in his possession in Colorado.

15. On July 16th, 2013, The University of Colorado police department made contact with PELLOSKI and secured a Dell laptop that was in his possession so that it could be shipped to your affiant in Ohio. The laptop is a Dell model PT135. Your affiant received the Dell laptop computer on Friday, July 19, 2013.

16. Pursuant to a federal search warrant that was issued on Friday, July 19, 2013, your affiant initiated complete forensic examinations of all of the computers and digital media that were seized from the PELLOSKI residence, as well as the Dell laptop computer that was recovered by the University of Colorado police department. Although the forensic examinations of these items are ongoing, your affiant has discovered significant evidence that Christopher PELLOSKI downloaded numerous images and videos depicting minors engaged in explicit sexual activity via the internet. Specifically, the forensic examination has revealed the presence of 25 images of child pornography and more than one hundred link files indicating access to files with names

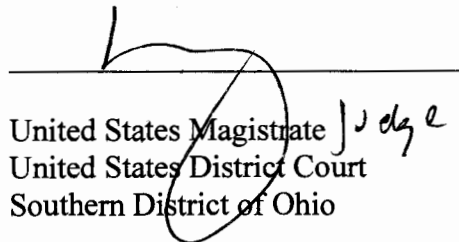
typically associated with child pornography on the HP Pavilion desktop computer that was seized from PELLOSKI'S bedroom. One of the images that your affiant viewed is a widely distributed child pornography image, and the victim depicted in this image has been previously identified by law enforcement. The Dell laptop was similarly found to contain artifacts indicative of child pornography, including file paths, file names and link files associated with child pornography. Link files show that a user of the computer has recently accessed and viewed the file. Some of the file paths and link files were recovered from the default folder on the computer, which is utilized by the peer-to-peer programs to download and share files, thus indicating that the files that PELLOSKI accessed were obtained from the internet.

17. Based upon the foregoing evidence, your affiant submits that there is probable cause to believe that Christopher PELLOSKI did receive visual depictions of minors engaged in explicit sexual activity via a means or facility of interstate commerce, that is the internet, in violation of Title 18 USC 2252(b). Therefore, your affiant respectfully requests this Court issue a criminal complaint.



John L. Priest,
Task Force Officer
Homeland Security Investigations

Sworn to and subscribed before me this 24th day of July, 2013.



United States Magistrate Judge
United States District Court
Southern District of Ohio